REMARKS

Claims 1-6, 8-32, and 34-50 remain in this application, as amended above. Applicants respectfully request reconsideration and review of the application in view of the foregoing amendments and following remarks.

At the outset, Applicants acknowledge with appreciation the courtesy of the Examiner in conducting the telephonic interview on June 16, 2005. The Applicants discussed the foregoing amendments with the Examiner during the interview, and the Examiner acknowledged that the amended claims distinguished over the prior art of record.

The Examiner rejected Claims 1-27 and 36 under 35 U.S.C. § 112, second paragraph, as indefinite. While Applicants consider the claims sufficiently definite as originally presented, Applicants have made certain amendments that are believed to further clarify the meaning of the claims. All claims present in the application are now considered sufficiently definite.

With respect to Claim 5, Applicants consider the "universal location" to be sufficiently clear and not inconsistent with Claim 1 on which it ultimately depends. It should be appreciated that Claim 1 recites that the "location identity data ... defines *at least* a specific geographic location," thereby leaving open the possibility of the "location identity data" defining a "universal location" in addition to the "specific geographic location."

Before addressing the merits of the rejections based on prior art, Applicants provide the following brief description of the invention. The invention pertains generally to the encryption of data using location information in order to limit access to the information to a particular location. In an embodiment of the invention, plaintext data is first encrypted using a random data encrypting key that is generated at the time of encryption. The data encrypting key is then encrypted (or locked) using a location value and a key encrypting key. This is a two-step process that involves using the location

value to modify the data encrypting key to produce a location-modified data encrypting key. The location-modified data encrypting key is then encrypted with the key encrypting key. The encrypted location-modified data encrypting key and the ciphertext data is then transmitted to the receiver. The receiver both must be at the correct location and must have a copy of a corresponding key decrypting key in order to decrypt the encrypted location-modified data encrypting key and extract the data encrypting key from the location-modified data encrypting key. After the data encrypting key is decrypted (or unlocked), it is used to decrypt the ciphertext. If an attempt is made to decrypt the data encrypting key at an incorrect location or using an incorrect key decryption key, the decryption will fail. In addition, the encrypted data encrypting key or ciphertext optionally may be altered so that it becomes impossible to ever decrypt that particular ciphertext. The data encrypting key may also be encrypted in a manner that it can only be accessed at a certain time or during a specific time frame.

In accordance with another embodiment of the invention, the ciphertext data can be routed through one or more intermediary distributors before being transmitted to a final receiver. One method for doing this involves encrypting the data encrypting key with a location value and key encrypting key for a particular distributor. The distributor then decrypts the data encrypting key and re-encrypts it using a location value and key encrypting key for the receiver. Another method for routing the ciphertext through a distributor involves encrypting the data encrypting key first with a location value and key encrypting key for the final receiver and then with a location value and key encrypting key for the distributor. The distributor removes its layer of encryption from the key before forwarding it to the receiver. If there are multiple distributors, the data encrypting key is successively encrypted with a location value and key encrypting key for each distributor on the path, but in reverse order. As the encrypted key is passed from one distributor to the next, each distributor removes its layer of encryption. With this method, none of the distributors can decrypt the data encrypting key because it remains encrypted with the location value and key encrypting key for the final receiver. Thus,

the distributors cannot access the plaintext. This method also forces the ciphertext to follow a particular path to the receiver.

As will be further described below, none of the references of record use location data to modify a data encrypting key before it is encrypted with a key encrypting key. Because location is integrated into the key encryption process, a receiver absolutely must have the correct location in order to acquire the data encrypting key and then decrypt the data. Applicants have amended the claims to clarify these aspects of the invention and put the claims in better form for allowance.

The Examiner rejected Claims 1-4, 6-16, 28-31, 32-39, and 45-47 under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Murphy. This rejection is respectfully traversed.

Menezes provides a general text showing the current state of cryptography. The Examiner acknowledges that "Menezes does not explicitly teach using information derived from a location identity attribute that defines at least a specific geographic location in the encryption process." Applicants concur with this statement, and further maintain that no other references of record make up for this deficiency of Menezes.

Murphy is directed to the control over decryption of encrypted signals based on the location where the decryption is performed. More particularly, Murphy discloses a decryption module that includes a Satellite Positioning System (SATPS) antenna and signal receiver/processor. The decryption module (1) determines the present location of the antenna, (2) compares the present location with a licensed site location stored in the receiver/processor for the particular decryption chip, and (3) shuts down or disables the signal decryption routine if the SATPS-determined present location of the antenna does not match the licensed site location. As shown in Fig. 2, an activation switch 31i is coupled to the decryption chip 15i, and will deactivate the decryption chip if the antenna is determined to not be in the proper location. The encrypted signals (ES) can only be decrypted when the decryption chip is activated.

As a fundamental matter, Murphy does not use location data in the encryption of

keys used to protect the underlying digital information. Murphy is directed to a one-to-many communication system in which the same encrypted signals are sent to many users. There is nothing distinctive about the encrypted signals that reflects a transformation using data defining a specific geographic location. In fact, the encrypted signals themselves have no relation to the location information whatsoever. Instead, Murphy uses location information only to determine whether to activate the decryption chip. The SATPS location signal is compared to location information that is previously stored in the receiver, and which has nothing to do with the encrypted signals. Notably, this determination occurs whenever the set-top box (i.e., receiver) is turned on or after the power supply is interrupted (see col. 8, lines 6-24 and 46-62), i.e., without any consideration of the encrypted signals.

Applicants respectfully submit that Murphy fails to make up for the deficiency of Menezes. Murphy teaches only the use of location as a gate-keeper function in determining whether or not to activate the decryption chip. Murphy does not use location to transform the information or keys being communicated. In fact, Murphy contains no discussion of key selection, generation or usage. Thus, a combination of Menezes and Murphy would at most yield a conventional encryption system in which location is used solely to activate the decryption circuitry. The only teaching to use location information to transform the information or decryption keys comes from the present patent application.

More particularly, the proposed combination of references fails to suggest or disclose, *inter alia*, the step of "modifying the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key," as defined in Claim 1. Moreover, the proposed combination fails to suggest or disclose, *inter alia*, the step of "encrypting said location-modified data encrypting key using a key encrypting key to produce an encrypted location-modified data encrypting key," as further defined in Claim 1. Claim 28 contains similar limitations that are neither suggested or disclosed by the proposed combination. Neither reference

suggests or discloses the desirability of using location identity data to modify a data encrypting key. Likewise, the proposed combination of references fails to suggest or disclose, *inter alia*, the step of "generating a key decrypting key using location identity data that defines a specific geographic location of said apparatus," as defined in Claim 45. Neither reference suggests or discloses the desirability of using location identity data to generate a key decrypting key.

In view of the absence of any teaching or suggestion of these claim limitations, a *prima facie* case of obviousness cannot be sustained. The rejection of these claims should therefore be withdrawn.

The claims dependent upon independent Claims 1, 28 and 45 contain additional limitations not suggested or disclosed by the combination of references. For example, Claims 10, 12, and 36 all include limitations directed to a "shape parameter defining a shape of a region encompassing said specific geographic location." None of the references of record disclose anything corresponding to a "shape parameter." With respect to these particular limitations, the Examiner states "the proximity value inherently corresponds to a zone that encompasses the location," and "a proximity value reads on a shape parameter." Applicants are unclear how these conclusions support a finding of obviousness. Nevertheless, the Examiner fails to show how these claimed features are disclosed by the prior art.

The Examiner rejected Claims 18-19 and 39 under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Murphy and in further view of Schneier. This rejection is respectfully traversed.

Like Menezes, Schneier provides a general text showing the current state of cryptography. The Examiner cites Schneier merely for its disclosure of pseudo-random number generation of a data encrypting key. Otherwise, Schneier fails to make up for the deficiencies of the other references discussed above, and more specifically, does not use location data to transform the information or keys being communicated. This ground of rejection should therefore be withdrawn.

With respect to Claim 19, the Examiner acknowledges that the references fail to disclose use of GPS signals to seed the pseudo-random number generator, but asserts without support that such teaching would be obvious. Applicants respectfully disagree. Since the references do not teach or suggest any use of location to transform the information or keys, there would be no motivation by persons skilled in the art to use GPS signals for such a purpose. To the contrary, the motivation for using GPS signals for this purpose comes directly from the use of location data to transform the information or keys, as taught by the present invention.

The Examiner rejected Claims 5, 21-27 and 41-44 under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Murphy and Schneier, and further in view of Shibata et al. This rejection is respectfully traversed.

Shibata et al. discloses a system for communicating encrypted information, and includes a cipher key table in which a plurality of cipher keys are stored. Otherwise, Shibata fails to make up for the deficiencies of the other references discussed above, and more specifically, does not use location data to transform the information or keys being communicated. This ground of rejection should therefore be withdrawn.

With respect to Claim 5, the Examiner asserts without support that it would have been obvious to include a universal location within the location value. Applicants respectfully disagree. Within the context of a location-based encryption system, it is counter-intuitive to provide a universal location value that effectively defeats the purpose of encrypting data for use only at a specific location. Insofar as none of the references of record disclose the use of location data to transform the information or keys being communicated, Applicants maintain that it would not be obvious to have the location data encompass a universal location in addition to a specific location.

The Examiner rejected Claims 1, 11, 16-17, 20, 28, 37-38, 40, 45 and 48 under 35 U.S.C. § 103(a) as unpatentable over Inoue et al. in view of Murphy. This rejection is respectfully traversed.

Inoue discloses a packet processing system that eliminates redundant

encryption/decryption of message packets passing through intermediate agents between sender and recipient. According to the reference, when relaying encrypted packets of digital information, each node in the relay will decrypt and then re-encrypt the packet. For ease of understanding, this communication may be described as E-D-E-D for a message passing through a single relay point and being encrypted (E) and decrypted (D) twice. For a message passing through two relay points, the communication would be E-D-E-D-E-D.

The reference discloses a relay encryption process in which adjacent senders and receivers share a master key that can be used for encryption and decryption, and that is kept in a master key database. The packet is first encrypted with a packet encrypting key that is included with the encrypted packet to decrypt the data or message portion of the packet. Rather than decrypt and encrypt the entire message at each relay point, Inoue uses a second encrypting key to encrypt the packet encrypting key. At each relay point, the decryption and subsequent encryption is performed only on the packet encrypting key, and not on the entire packet. The second encrypting key is shared between a relay point and the previous node in their master key databases. Thus, a packet sent through two relay points to a recipient would appear as E-D1-E1-D2-E2-D, in which D1 and E1 are the decryption and encryption of the packet encrypting key by the first relay point, and D2 and E2 are the decryption and encryption of the packet encrypting key by the second relay point.

Notably, the Inoue communication method does not use location data to encrypt the packet encrypting key. In this respect, Inoue suffers from the same deficiency as Menezes and the other references. Murphy fails to make up for this deficiency, for substantially the same reasons set forth above.

Specifically, the proposed combination of references fails to suggest or disclose, *inter alia*, the step of "modifying the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key," as defined in Claim 1. Moreover, the proposed combination fails to

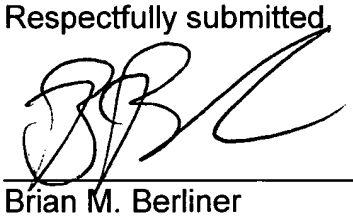
suggest or disclose, *inter alia*, the step of "encrypting said location-modified data encrypting key using a key encrypting key to produce an encrypted location-modified data encrypting key," as further defined in Claim 1. Claim 28 contains similar limitations that are neither suggested or disclosed by the proposed combination. Neither reference suggests or discloses the desirability of using location identity data to modify a data encrypting key. Likewise, the proposed combination of references fails to suggest or disclose, *inter alia*, the step of "generating a key decrypting key using location identity data that defines a specific geographic location of said apparatus," as defined in Claim 45. Neither reference suggests or discloses the desirability of using location identity data to generate a key decrypting key.

In view of the absence of any teaching or suggestion of these claim limitations, a *prima facie* case of obviousness cannot be sustained. The rejection of these claims should therefore be withdrawn.

In view of the foregoing, the Applicants respectfully submit that Claims 1-6, 8-32, and 34-50 are in condition for allowance. Reconsideration and withdrawal of the rejections is respectfully requested, and a timely Notice of Allowability is solicited. To the extent it would be helpful to placing this application in condition for allowance, the Applicants encourage the Examiner to contact the undersigned counsel and conduct a telephonic interview.

While the Applicants believe that no fees are due in connection with the filing of this paper, the Commissioner is authorized to charge any shortage in the fees, including extension of time fees, to Deposit Account No. 50-0639.

Respectfully submitted,



Date: June 17, 2005

Brian M. Berliner
Attorney for Applicants
Registration No. 34,549

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000